Amendments to the Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1. (Currently Amended) A method for providing access management through use of a plurality of server machines associated with different locations, said method comprising ~~the acts of~~:

~~(a)~~ receiving, at a first server machine of the plurality of server machines, an access request to access a secure item from a first client machine at a first location;

~~(b)~~ authenticating a user of the first client machine at the first location;

~~(c)~~ authenticating the first client machine;

~~(d)~~ upon successful authentication of the user and successful authentication of the first client machine ~~in steps (b) and (c)~~, retrieving at the first server machine a user key permitting access to an encrypted sub-header of the secured item, the encrypted sub-header including access rules for the secured item, the sub-header corresponding to the user or to a group to which the user belongs;

~~(e)~~ permitting access to the secure item via the first location when said authenticating of the user and authenticating of the first client machine ~~(b) and (c)~~ are successful, and further when allowed by the access rules;

~~(f)~~ permitting access to the secure item via the first server machine when said permitting access to the secure system via the first location ~~(e)~~ permits the user to gain access to the secure item from the first location; and

~~(g)~~ preventing access to the secure item via the first server machine when said permitting access to the secure system via the first location ~~(e)~~ does not permit the user to gain access to the secure item from the first location.

2. (Currently Amended) The method as recited in claim 1, wherein said permitting access to the secure system via the first location ~~(e)~~ comprises:

~~(e1)~~ obtaining access privileges associated with the user to determine at least one or more permitted locations for the user; and

~~(e2)~~ determining whether the user is permitted to gain access to the secure item from the first location based on the permitted locations associated with the user.

3. (Currently Amended) The method as recited in claim 1, wherein, when permitted by said permitting access to the secure system via the first location ~~(e)~~, allowing access to the secure item from the first location via the first client machine and the first server machine.

4. (Currently Amended) The method as recited in claim 1, wherein, when permitted by said permitting access to the secure item via the first server machine ~~(f)~~, allowing access to the secure item from the first location via the first client machine and the first server machine.

5. (Currently Amended) The method as recited in claim 1, further comprising ~~the acts of~~:

~~(h)~~ ——preventing access to the secure item via any of the server machines other than the first server machine when said permitting access to the secure item via the first server machine ~~(f)~~ permits the user to gain access to the secure item from the first location.

6. (Currently Amended) The method as recited in claim 1,

wherein said permitting access to the secure system via the first location ~~(e)~~ comprises determining whether the user is permitted to gain access to the secure item via the first client machine and the first server machine, and

wherein said permitting access to the secure item via the first server machine ~~(f)~~ operates to permit the user to gain access to the secure item via the first client machine and the first server machine when said permitting access to the secure system via the first location ~~(e)~~ determines that the user is permitted to gain access to the secure item via both the first client machine and the first server machine.

7. (Currently Amended) The method as recited in claim 1,

wherein said permitting access to the secure system via the first location ~~(e)~~ comprises determining whether the user is permitted to gain access to the secure item via the first server machine, and

wherein said permitting access to the secure item via the first server machine ~~(f)~~ operates to permit the user to gain access to the secure item via the first server machine when said permitting access to the secure system via the first location ~~(e)~~ determines that the user is permitted to gain access to the secure item via the first server machine.

8. (Currently Amended) The method as recited in claim 1,

wherein said permitting access to the secure system via the first location ~~(e)~~ comprises determining whether the user is permitted to gain access to the secure item via the first client machine, and

wherein said permitting access to the secure item via the first server machine ~~(f)~~ operates to permit the user to gain access to the secure item via the first client machine when said permitting access to the secure system via the first location ~~(e)~~ determines that the user is permitted to gain access to the secure item via the first client machine.

9. (Currently Amended) The method as recited in claim 1, further comprising ~~the acts of~~:

~~(h)~~ ——preventing the user from gaining access to the secure item via any of the server machines other than the first server machine when said permitting access to the secure system via the first location ~~(e)~~ determines that the user is permitted to gain access to the secure item from the first location.

10. (Currently Amended) The method as recited in claim 9, wherein said preventing ~~(h) of~~ the user ~~to gain~~ from gaining access to the secure item via any of the other server machines comprises reconfiguring at least any of the other server machines that previously permitted the user to gain access to the secure item therethrough.

11. (Currently Amended) The method as recited in claim 10, wherein said permitting ~~(f) of the user to gain~~ access to the secure item via the first server machine comprises reconfiguring the first server machine to permit access by the user to the secure item via the first server machine.

12. (Currently Amended) The method as recited in claim 11, wherein said permitting access to the secure system via the first location ~~(e)~~ comprises:

~~(e1)~~ obtaining access privileges associated with the user to determine at least one or more permitted locations for the user; and

~~(e2)~~ determining whether the user is permitted to gain access to the secure item from the first location based on the permitted locations associated with the user.

13. (Currently Amended) The method as recited in claim 1, wherein said permitting ~~(f) of the user to gain~~ access to the secure item via the first server machine

comprises reconfiguring the first server machine to permit access by the user to the secure item via the first server machine.

14. (Previously Presented) The method as recited in claim 1, wherein the secure item is a secured file, the secured file having a format that comprises a header including security information as to who and how access to the secure item is permitted; an encrypted data portion including data of the secured file encrypted with a file key according to a predetermined cipher scheme, and wherein the header is attached to the encrypted data portion to generate the secured file.

15. (Previously Presented) The method as recited in claim 14, wherein the security information in the header of the secured file facilitates the restricted access to the secured file.

16. (Previously Presented) The method as recited in claim 15, wherein the security information in the header of the secured file points to or includes the access rules and a file key.

17. (Previously Presented) The method as recited in claim 14, wherein the security information is encrypted with a user key associated with the user.

18. (Previously Presented) The method as recited in claim 14, wherein the security information includes the file key and access rules to the restricted access to the secured file.

19. (Previously Presented) The method as recited in claim 18, wherein the file key is retrieved to decrypt the encrypted data portion in the secured file when access privilege of the user is within access permissions by the access rules.

20. (Previously Presented) The method as recited in claim 18, wherein the access rules are expressed in a markup language.

21. (Currently Amended) A method for providing access management through use of a distributed network of server machines, said method comprising ~~the acts of~~:

~~(a)~~ receiving, at a first server machine of the plurality of server machines, an access request to access a secure item from a first client machine;

~~(b)~~ authenticating a user of the client machine;

~~(c)~~ authenticating the first client machine;

~~(d)~~ upon ~~successful~~ successfully authenticating the user and authenticating the first client machine ~~in step (b) and (c)~~, retrieving at the first server machine a user key permitting access to an encrypted sub-header of the secure item, the encrypted sub-

header including access rules for the secure item, the sub-header corresponding to the user or to a group to which the user belongs;

~~(e)~~ retrieving access privileges associated with the user;

~~(f)~~ determining whether the user is permitted to gain access to the secure item via the first server machine based on the access privileges and access rules when said authenticating the user and said authenticating the first client machine ~~(b) and (c)~~ are successful;

~~(g)~~ permitting access to the secure item via the first server machine when said determining whether the user is permitted to gain access to the secure item via the first server machine ~~(f)~~ determines that the user is permitted to gain access to the secure item via the first server machine; and

~~(h)~~ preventing access to the secure item via the first server machine when said determining whether the user is permitted to gain access to the secure item via the first server machine ~~(f)~~ determines that the user is not permitted to gain access to the secure item via the first server machine.

22. (Currently Amended) The method as recited in claim 21, further comprising ~~the acts of~~:

~~(i)~~ preventing access to the secure item via any of the server machines other than the first server machine when said determining whether the user is permitted to gain access to the secure item via the first server machine ~~(e)~~ determines that the user is permitted to gain access to the secure item via the first server machine.

23. (Currently Amended) The method as recited in claim 21,

wherein said determining whether the user is permitted to gain access to the secure item via the first server machine ~~(f)~~ further determines whether the user is permitted to gain access to the secure item via the first client machine, and

wherein said permitting access to the secure item via the first server machine ~~(g)~~ operates to permit the user to gain access to the secure item via the first client machine and the first server machine when said determining whether the user is permitted to gain access to the secure item via the first server machine ~~(f)~~ determines that the user is permitted to gain access to the secure item via both the first client machine and the first server machine.

24. (Currently Amended) The method as recited in claim 23, further comprising ~~the acts of~~:

~~(i)~~ preventing access to the secure item via any of the server machines other than the first server machine when said determining whether the user is permitted to gain access to the secure item via the first server machine ~~(f)~~ determines that the user is permitted to gain access to the secure item via the first server machine.

25. (Currently Amended) The method as recited in claim 24, wherein said preventing ~~(i) of~~ access to the secure item via any of the other server machines comprises reconfiguring at least any of the other server machines that previously permitted the user to gain access to secure items therethrough.

26. (Currently Amended) The method as recited in claim 25, wherein said permitting ~~(g) of~~ access to the secure item via the first server machine comprises reconfiguring the first server machine to permit access by the user to the secure item via the first server machine.

27. (Currently Amended) The method as recited in claim 21, wherein said permitting ~~(g) of the~~ access to the secure item via the first server machine comprises reconfiguring the first server machine to permit access to the secure item via the first server machine.

28. (Previously Presented) The method as recited in claim 21, wherein the secure item is a secured file, the secured file having a format that comprises a header including security information as to who and how access to the secured file is permitted; an encrypted data portion including data of the secured file encrypted with a file key according to a predetermined cipher scheme, and wherein the header is attached to the encrypted data portion to generate the secured file.

29. (Previously Presented) The method as recited in claim 28, wherein the security information in the header of the secured file facilitates the restricted access to the secured file.

30. (Previously Presented) The method as recited in claim 28, wherein the security information is encrypted with a user key associated with the user.

31. (Previously Presented) The method as recited in claim 28, wherein the security information includes the file key and access rules to the restricted access to the secured file.

32. (Previously Presented) The method as recited in claim 28, wherein the file key is retrieved to decrypt the encrypted data portion in the secured file when access privilege of the user is within access permissions by the access rules.

33. (Previously Presented) The method as recited in claim 31, wherein the access rules are expressed in a markup language.

34. (Currently Amended) A tangible computer-readable medium ~~including at least computer program code~~ having computer-executable instructions stored thereon that, if executed by a computing device, cause the computing device to perform a method for providing access management to secured content through use of a plurality of server machines associated with different locations, ~~by a~~ the method comprising:

receiving, at a first server machine of the plurality of server machines, an access request to access a secure item from a first client machine at a first location;

authenticating a user of the first client machine at the first location;

authenticating the first client machine;

retrieving at the first server machine a user key permitting access to an encrypted sub-header of the secured item, the encrypted sub-header including access rules for the secure item upon authentication of the user and the first client machine, the sub-header corresponding to the user or to a group to which the user belongs;

determining whether access to the secure item via the first location is permitted when said computer program code for authenticating the first client machine and the user are successful, and further based on the access rules;

permitting access to the secure item via the first server machine when said computer program code for determining determines that the user is permitted to gain access to the secure item from the first location; and

preventing access to the secure item via the first server machine when said computer program code for determining determines that the user is not permitted to gain access to the secure item from the first location.

35. (Currently Amended) A tangible computer-readable medium ~~including at least computer program code~~ having instructions stored thereon for providing access management through use of a distributed network of server machines, ~~said computer readable medium~~ the instructions comprising:

~~computer program code~~ instructions for receiving, at first server machine of the plurality of server machines, an access request to access a secure item from a first client machine;

~~computer program code~~ instructions for authenticating a user of the client machine;

~~computer program code~~ instructions for authenticating the first client machine;

~~computer program code~~ instructions for retrieving at the first server machine a user key permitting access to an encrypted sub-header of the secured item, the encrypted sub-header including access rules for the secure item upon authenticating of the user and the first client machine, the sub-header corresponding to the user or to a group to which the user belongs;

~~computer program code~~ instructions for retrieving access privileges associated with the user;

~~computer program code~~ instructions for determining whether the access to the secure item via the first server machine is permitted based on the access privileges and access rules when said computer program code for authenticating the first client machine and the user are successful;

~~computer program code~~ instructions for permitting access to the secure item via the first server machine when said computer program code for determining determines that the user is permitted to gain access to the secure item via the first server machine; and

~~computer program code~~ instructions for preventing access to the secure item via the first server machine when said computer program code for determining determines that the user is not permitted to gain access to the secure item via the first server machine.

36. (Currently Amended) An access control system that restricts access to a secure item, said system comprising:

a central server having a server module that provides overall access control; and

a plurality of local servers, each of said servers including a local module that provides local access control,

wherein the access control, performed by said central server or said local servers, operates to permit or deny access requests to secured items by requestors, and

wherein, based on information stored in an encrypted sub-header of a secure item, the sub-header corresponding to the given requestor or to a group to which the requestor belongs, a given requestor, permitted to access the secure item through one or more of said local servers, is only able to access the secure item using only a single one of said local servers or the central server such that the given requestor is only permitted to access the secure item through at most one of said local servers at a time.

37. (Previously Presented) The access control system as recited in claim 36, wherein said access control system couples to an enterprise network to restrict access to the secure item, which comprises a secured file, stored therein.

38. (Previously Presented) The access control system as recited in claim 37, wherein the access requests are at least primarily processed in a distributed manner by said local servers.

39. (Previously Presented) The access control system as recited in claim 38, wherein when the access requests are processed by said local servers, the requestors gain access to the secured files without having to access said central server.

40. (Previously Presented) The access control system as recited in claim 37, wherein the local module is a copy of the server module so any of the local modules operate independently of said central server and other of said local servers.

41. (Previously Presented) The access control system as recited in claim 37, wherein the local module is a subset of the server module.

42. (Previously Presented) The access control system as recited in claim 37, wherein access permissions for said local servers is dynamically configured to pass a

requestor from one of said local servers to another of said local servers, thereby enabling access control to be performed by the another of said local servers such as when the location of the requestor changes.

43. (Previously Presented) The access control system as recited in claim 37, wherein the secured files are secured by encryption of the secure item.

44. (Previously Presented) The access control system as recited in claim 37, wherein the secure item is secured by encryption.